Comment Report

STATEWIDE POLICY – COMPUTER SECURITY INCIDENT MANAGEMENT

FEBRUARY 11, 2009

Scope:

This report contains the comments and responses for the statewide review of the *Statewide Policy: Computer Security Incident Management* and its associated instruments, which was available for review January 8th to 30th, 2009.

Executive Summary

The purpose of this document is to:

1. Publish received comments,
2. indicate status of proposed changes, and
3. respond to each comment.

Comments were received from five agencies, over the period of January 21st through February 3rd. The comments and feedback appear to emanate from the technical audience, and their comments were in the following areas:

1. Technical errors in the documentation, such as non-functioning URLs. These have been corrected.
2. Proposed prose changes in the requirements. These have largely been rejected because the changes would materially alter the requirements. They are addressed herein.
3. Questions regarding supporting services from ITSD. These are service issues, not statewide policy issues, and have not been included herein. The service issues have been referred to ITSD for disposition.
4. Comments regarding details of referenced documents. These have been addressed herein.

5. Comments regarding implementation; specifically service provider relationships and funding. These have been addressed herein.

The respondents did not appear to include agency policy-makers - those individuals nominally responsible for implementing policy (i.e., directors, administrators, etc.); and *policy-level* concerns were not detected within the comments. The upshot being that we are aware of no policy-maker issues stemming from this policy.

The recommendation from the policy manager to the State of Montana Chief Information Officer is to approve the policy based on the response herein.

Comments/Feedback with Response

Item	Comment/Suggestion	Response/ Disposition	Status
1.	**COMMENT:** Statewide Standard: Computer Security Incident Management The Statewide Standard: Computer Security Incident Management, has a broken link IV Definitions - Statewide Information system Policies and Standards Glossary.	**RESPONSE:** The URL has been repaired.	Complete
2.	**COMMENT:** Statewide Standard: Computer Security Incident Management The Statewide Standard: Computer Security Incident Management, under section III. Scope, second paragraph - the first paragraph states that the scope is for a statewide standard for the information systems and assets managed or controlled by each agency. Then the second paragraph states systems managed or hosted by third parties. Does "third parties" include ITSD? Statewide Policy: Computer Security Incident Management, section V. Scope has the same third party reference.	**RESPONSE:** The Department of Administration is a "third party" service provider to the agencies. By *convention*, ITSD is a service provider *through* DOA for services cited within the reference. Reference §2-17-512(1)(m) MCA, et seq. From the FISMA/NIST perspective, any party that provides your agency with information system/security services is considered a third party (or "external" party/provider). As an example, Google, Microsoft, SunGard, or ITSD are third parties if your agency obtains services from them.	Complete
3.	**COMMENT:** Statewide Standard: Computer Security Incident Management	**RESPONSE:** The suggested changes to the prose are rejected because the changes	Change rejected.

Item	Comment/Suggestion	Response/ Disposition	Status
	The respondent made several edits of the prose within the standard, paragraph V.	amount to the same meaning with different words and sentence structure. However, under the FISMA/NIST framework, the agency is free to alter the vernacular within their own (local) version of the standard, to include adding local requirements beyond (but not negating) the statewide standard requirements (which define "baseline" requirements for the state). Reference NIST SP800-53 Revision 2, Appendix F Security Control Catalog, Incident Response 1 (IR-1) Control (page F-38).	
4.	**COMMENT:** Statewide Standard: Computer Security Incident Management Statewide Standard: Computer Security Incident Management: The respondent deleted the following sentence from paragraph V.B.2.a: ~~*The results of the risk assessment shall determine any changes in the level of process, standards and controls.*~~	**RESPONSE:** The suggested deletion of this sentence is rejected because it would materially alter the requirement. However, a review of the sentence against FISMA/NIST documentation revealed an inaccuracy, and the sentence is now changed to: *After review of the risk assessment(s), agency management shall determine any changes in the level of process, standards and controls.*	Changed
5.	**COMMENT:** Statewide Standard: Computer Security Incident Management The Department is concerned about the amount of resources that will be required to achieve compliance with these policies, especially in a smaller department and/or division where resources and skill sets are not in place and existing resources are at capacity.	**RESPONSE:** These requirements stem from the Legislature (via §2-17-534 MCA and §2-15-114 MCA) and the Legislature is the appropriate forum to address funding of statutory mandates.	No Change
6.	**COMMENT:** Statewide Standard: Computer Security Incident Management c. In the event ITSD provides hosting services to agencies, and ITSD is unable to meet these standards, is the agency or ITSD required to pursue exception approval? Who retains responsibility and/or liability in these	**RESPONSE:** We are aware of no vehicle to transfer statutory requirements, such as the requirements of §2-17-534 MCA and §2-15-114 MCA. From the FISMA/NIST perspective, obtaining services from a service provider such as Google, Microsoft, SunGard, or ITSD does not relieve the customer from its security responsibilities. NIST expects service agreements to address	No Change

Item	Comment/Suggestion	Response/ Disposition	Status
	situations?	these issues and provide assurance that the service provider is fully supporting customer requirements – including security requirements; either directly or indirectly. (But it is sound practice to obtain legal advice regarding requirements and their impact on agreements.)	
7.	**COMMENT:** Statewide Policy: Computer Security Incident Management **Section III Policy Statement** We recommend that besides listing the name of the document and providing the link, that you reference the publication and revision number so there is no confusion if one is working off printed documentation.	**RESPONSE:** Please advise where this has not been done, and it will be corrected.	Pending
8.	**COMMENT:** Statewide Standard: Computer Security Incident Management Standard **Item V. Requirements and Specifications** Item B. Performance Requirements -- Are both options (a and b) tied to the September 1, 2010 implementation date? If we focus on item 2b and implement the low-impact baseline, when would we be forced to move through moderate-impact and high-impact baselines?	RESPONSE: Yes, the implementation date is applicable to both implementation options. Under this approach, agencies have a choice; but have to implement by that date. When an agency moves to higher levels of controls (i.e., "moderate-impact" or "high-impact") is an agency *business* decision, which by policy shall be based upon the results of the agency's actions vis-a-vis the NIST Risk Management Framework.	No Change
9.	**COMMENT:** Statewide Standard: Computer Security Incident Management Standard **Item VI. Compliance** The requirement is that we meet the criteria in Annex A, however Annex A calls in Publication 199 which talks about the categorization of impact for your various systems, implying that	**RESPONSE:** It is the data, and its processed form – information, that is the object of the protection measures. Reference §2-15-114 MCA.	No Change

Item	Comment/Suggestion	Response/ Disposition	Status
	we have to go through all of our systems and apply this categorization and then implement the appropriate security level for that system. This is in conflict with only completing the low-impact requirements in item 2b as mentioned in the preceding paragraph. This gets us back to the question as to what is really being required by this policy.	The FISMA/NIST framework requires categorization at the heart of *all* data/information security. As a result, all risk assessment processes and security control selection is based on a common *categorization* of the risk related to the operation and use of information and information systems, as defined within the FIPS 199 and FIPS 200 standards. Hence, these standards are the basis for categorizing information *with a standard definition of levels of impact to the organization, for all control selection*.	
10.	**COMMENT:** Statewide Standard: Computer Security Incident Management In Annex A - *Section IV General Incident Response Compliance Criteria* - we are required to implement either a) the appropriate impact baseline or b) without an assessment, implement the levels of controls based upon the schedule requirements of the Standard. Does this again take us back to the previous paragraph and there is no further schedule beyond the low-impact baseline implementation of 9/1/2010?	**RESPONSE:** Correct. This compliance criteria mirrors the requirement within the parent standard.	No Change
11.	**COMMENT:** Statewide Standard: Computer Security Incident Management Also in this section of Annex A it refers to meeting the *General Incident Response Compliance Criteria* and points us to the Computer Security Incident Handling Guide (pub 800-61) without any specifics. Are we to focus on only Section 3 "Handling an Incident" for general guidelines or is this just a	**RESPONSE:** The reason that Annex A is not labeled “requirements” is to honor the spirit and reality of federalism by avoiding prescriptive and proscriptive policies, and to respect agency capacity to manage their affairs and make informed decisions about their aggregate mix of requirements; hence the statewide policy/standard focus on high-level requirements. As “compliance criteria,” the agency gets to make its own decisions whether or not to comply; and how. However, we would expect auditors to ask two	No Change

Item	Comment/Suggestion	Response/ Disposition	Status
	nice way of saying do everything in the 147 page document? Further details within Section IV *General Incident Response Compliance Criteria* (sections A-G) point us to approximately 18 pages within the 800-61 publication. If we focus on that criteria will we be in compliance with the 'general controls'?	questions: 1. "Are you using NIST SP800-61 for guidance?" 2. "Have you implemented the specific controls listed in Annex A?" Also as a forewarning, Annex A has some relation to probable *requirements* that may originate from external benefactors, such as the Federal Government. If your agency has federal "strings," the wise course of action is to understand the compliance associated with those strings.	
12.	**COMMENT:** Statewide Standard: Computer Security Incident Management In Annex A - *Section V Ratings of Incidents* it references Continuity of Government Plan. <Our agency's> plan includes categories of incidents related to physical incidents more so than security incidents. For example, at level I (isolated incidents that are routinely handled by local authorities), level II (incidents that exceed the capacity of available local resources from the impacted area), and level III (catastrophic events that require massive amounts of resources from local, state and federal govts) the security definitions would not be good match to the level of involvement. Are we to incorporate security into those same categories or work with our COOP planner to devise more relevant security incident categories to meet the compliance requirements?	**RESPONSE:** The standard (and NIST) does not address how agencies categorize *specific incidents* or *what types* of incidents shall be defined, because this will vary by agency. (Although NIST SP800-61 contains guidance within the information security context.)	No Change